



BSI Standards Publication

Health informatics — Cybersecurity framework for telehealth environments

Part 2: Cybersecurity reference model of telehealth

National foreword

This Published Document is the UK implementation of ISO/TS 6268-2:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 27929 0

ICS 35.240.80

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2025.

Amendments/corrigenda issued since publication

Date	Text affected



Technical Specification

ISO/TS 6268-2

Health informatics — Cybersecurity framework for telehealth environments —

Part 2: Cybersecurity reference model of telehealth

*Informatique de santé — Cadre en matière de cybersécurité pour
les environnements de télésanté —*

Partie 2: Modèle de référence de cybersécurité pour la télésanté

**First edition
2025-05**



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	2
4 Cybersecurity reference model of telehealth service	2
4.1 General	2
4.2 Components of the cybersecurity reference model of telehealth service	3
5 Telehealth service activities and threats	4
5.1 General	4
5.2 Encounter	4
5.2.1 Description	4
5.2.2 Threats	4
5.3 Observation	5
5.3.1 Description	5
5.3.2 Threats	5
5.4 Intervention	5
5.4.1 Description	5
5.4.2 Threats	6
6 Security level of telehealth service	6
6.1 Cybersecurity, safety and remote communication	6
6.2 The scheme of cybersecurity level in telehealth services	7
6.3 Methodology of defining security level in telehealth services	7
Annex A (informative) Use cases based on real-world telehealth in ISO 13131	9
Bibliography	12

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

A list of all parts in the ISO 6268 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Telehealth once provided a limited range of services to subjects of care in specific environments. However, the scope of telehealth services is rapidly expanding through advanced information and communication technologies (ICT) such as mobile-based, cloud-based and other network-based applications. Additionally, emerging global pandemics have acutely increased the need to diagnose, prevent, monitor, treat or mitigate diseases and injuries without face-to-face, in-person contact between subjects of care and care providers, making telehealth a more commonly accepted medical practice.

These services are described as telehealth services because ICT are used to support healthcare activities. Telehealth services can include but are not limited to telemedicine, telecare, mHealth (healthcare supported by mobile devices), remote use of medical applications, tele-monitoring, tele-diagnostics and virtual care. Examples of health services include but are not limited to tele-pathology, tele-dermatology, tele-cardiology, tele-rehabilitation, tele-oncology and tele-orthopaedics. Healthcare activities that directly or indirectly support care recipients include but are not limited to teleconsultation, telephone advice, health alarm systems and health status monitoring at home. Telehealth services can support immediate healthcare activities using synchronous communications services such as a telephone or video conversation, or delayed health care activities using asynchronous communications services such as messaging services.

Furthermore, depending on the perspective, the subcategories of telehealth can also vary. Physicians might categorize telehealth by medical specialties, such as tele-neurology or tele-orthopaedics, while healthcare IT experts might focus on system topology and network configurations. When it comes to telehealth in cybersecurity, telehealth actors, interactions between each actor, data flow, service environment and technology should be considered. Therefore, establishing concepts and models of telehealth cybersecurity would be the first step to build a framework for cybersecurity in telehealth environment.

Telehealth cybersecurity concepts and models serve as a baseline for the analysis of cybersecurity threats and to determine countermeasures. Telehealth cybersecurity countermeasures need to consider not only technical aspects, but also management and physical approaches to operating telehealth services. This is because telehealth cybersecurity involves interactions between multiple actors situated in environments with different levels of cybersecurity. The cybersecurity policies and processes act as variables that influence the overall cybersecurity posture of telehealth.

People and physical requirements are addressed more deliberately in telehealth cybersecurity because participants beyond the network cannot be controlled. Actors on this side cannot even apply a band-aid to those on the other side. It will take time and effort to ensure that the quality of telehealth services matches that of general healthcare services. Actors need to account for variables that arise from not being able to see or directly address issues. Actors cannot know what is happening outside the camera's view. Physically occurring risks, such as break-in, theft, vandalism, disconnection and deception, are also critical issues that need to be addressed in the telehealth environment.

The cybersecurity framework for telehealth environment is structured as follows;

- Part 1: Overview and concepts;
- Part 2: Cybersecurity reference models of telehealth;
- Part 3: Cybersecurity requirements for telehealth.

This document is the second part in the ISO 6268 series and it covers a telehealth cybersecurity reference model of the overall security framework for systems and services applied to telehealth.